ISSN No:-2456-2165

Investigating the Impact of Cyber-Security on Sustainable Peace in Niger Delta Region of Nigeria Empirical Evidence

Tolulope Timothy BABARINDE
Department of Computer Engineering
Eastern Mediterranean University, North Cyprus, Turkey

Solomon Adejare BABARINDE
Department of Management and Accounting
Lead City University, Ibadan, Nigeria

Abstract:- The issues of cyber security has been ongoing in the exisiting literature. The Niger Delta Area in Nigeria has been characterized by unrest and other hostile activities. Hence, this study investigates how cybersecurity (measured in operational security, network security, application security and information security) will influence sustainable Peace in the Niger Delta. The cros sectional survey research design was employed in the study. Questionaiires were administered to six hundred and sixty-three (663) respondents from three states purposively selected from the Niger Delta area. The regression analysis shows that Operational Security, network security, application security and information security significantly influences sustainable peace. The study recommends that robust actions should be taken by stakeholders and government agencies in protecting critical cyber infrastructures in aother to achieve and sustain peace in the Niger Delta.

Keywoards:- *Cybersecurity, Niger Delta, Security, Sustainble Peace*

I. INTRODUCTION

The issue of security and how well a nation has to safeguard its national boundaries, citizens and economic assets has been a growing concern in domestic and local scenes. Zwilling et al. (2020) posit that cyber security procedures that help identify, minimise the risk and promote a viable environment with future cyber risks are included in a national strategic plan. A sustainable security environment is required to protect contemporary, technology-based civilisations and increase the nation's capacity to achieve its long term sustainable drive (Cain et al., 2018; Ajiji, 2017). Due to ever-increasing dangerous online actions, there is a rising need to improve cybersecurity, yet security innovations lag in Nigeria's emerging economies (Babayo et al., 2021). A plausible explanation for this situation could be that the country's policymakers are yet to see leverage the full benefits of technology in fighting crimes since they do not see the extent to which it could lead to a robust and vibrant economy (Sule, 2018).

The Global Cyber-security Index (GCI, 2019) lists cyberattacks as one of the world's leading risks leading to multi-billion-dollar corporate losses, notably if critical infrastructure such as banking and healthcare systems are hacked. Guiora (2017) posits that a lack of appropriate cybersecurity measures has resulted in two main roadblocks in the growth of information technology environments: resilience and credibility. This might have a negative impact on the information technology industry rather than fostering innovation (Koops, 2016). Technology-enhanced society will progressively lose faith, culminating in a catastrophic drop in growth if security measures are lacking or insufficient (Kshetri, 2019). Kosseff (2017) argues that cybersecurity encompasses a wide variety of topics, from creating a resilient infrastructure that can withstand assaults to developing techniques and systems that can assist in identifying threats and abnormalities, ensuring the robustness of a system and determining its reaction any attack.

To counter unconventional or nonmilitary challenges to domestic or foreign security, a paradigm shift of security discourse is being adopted by nations who are more security conscious and see insecurity of any type as a threat to national; development and economic expansion. (Cavelt and Wenge, 2019). Today's growing list of security threats, including maritime piracy, flood and drought damage to infrastructure and disease transmission, is compelling the countries, irrespective of their economic standing to reconsider the very basis of global security as we know it (Sule et al., 2019). Cybercrime is a constant threat to human life and national infrastructures, hence, cybersecurity (Buchanan, 2016). In the face of vulnerabilities and threats that might result in billions of dollars in property losses, currency theft, and the breakdown of crucial national facilities, countries are putting substantial effort into securing their cyberspace from hacks and malicious activities through operational security, network security, application security, information security and disaster recovery plan measures (Chukwuma & Mogon, 2018). These measures are used in various countries across the globe to reduce the incidence of cybercrime, causing billions of dollars in losses for private citizens, businesses, institutions, and governments alike (Antonucci 2017). While Nigeria is a growing country, it also deals with imminent threats on many fronts, including classic threats of war and unconventional difficulties like famine and the spread of terrorism. In light of this, the Nigerian government implemented a holistic cybersecurity set of recommendations in 2015, outlining the laws and national transformation program to provide a healthier cyber world for everybody (Babayo et al., 2021). Internet and cybersecurity are worldwide and present multiple vulnerabilities to all countries and investigations on Nigeria. However, there is a dearth of empirical findings on how cybersecurity could lead to sustainable peace in a volatile environment such as Nigeria.

As a result of the peculiarities of the Nigerian instance, research into cybersecurity and cybercrime is of particular importance in this country. Nigeria is Africa's most populated country and the world's most populous black nation. In terms of oil production, it ranks as the tenth most extensive state, while its population ranks as the world's seventh-largest. Policymakers and influential actors in the cybersecurity industry should be particularly concerned about the rapid growth of internet access in Nigeria since the country's inherent vulnerability will only worsen (Sule et al., 2019; Chukwuma & Mogon, 2018). This study fills a critical vacuum in Nigerian cybersecurity research by providing a detailed assessment of the cyber security that could drive sustainable development in the Niger Delta. With this report, we also provide policy recommendations for the government of Nigeria on how to strengthen the country's cybersecurity architecture in the Niger Delta. In addition to ensuring the safety and security of its population inside the nation-state, the state is responsible for protecting them from outside dangers. Cybersecurity and peacebuilding issues should be critical to any responsible administration. Cybersecurity has emerged as a current societal concern in the global social system. As a result, proponents of cybersecurity and peacebuilding initiatives argue that the focus of security should instead be on the person rather than on the state as a whole. Maintaining peace at the national, regional, and global levels requires a security strategy that puts people first. Adding credence to the above, Babayo et al. (2021) assert that the desire for safety and security is a universal issue that transcends geographical boundaries. To put it another way, the world's present state of safety and tranquillity is contradictory.

➢ *The following research questions were raised to address the research gap;*

- How does operational security drive sustainable peace in the Niger Delta region of Nigeria?
- In what way does network security influence sustainable peace in the Niger Delta region of Nigeria?
- What is the impact of application security on sustainable peace in the Niger Delta region of Nigeria?
- How does information security drive sustainable peace in the Niger Delta region of Nigeria?

II. CONCEPTUAL REVIEW

➢ *Cybersecurity and Measurements*

The exact meaning of cybersecurity has been debated by a wide range of persons, each having a distinct position on the matter. Beyond the scope of traditional criminal activity, cybercrime today threatens the peace and stability of all nations, even those with advanced technology capabilities like the developed economies (Diogenes & Ozkaya, 2018). Information and Communication Technology abuse for illicit or other objectives, particularly actions designed to damage the safety of countries valuable intelligence facilities, is vital to attaining global cyber security, as stated opined by Graham (2019). As a result, this study adds that international collaboration, investigation support, and uniform procedural and substantive measures are needed to deal with threats that emanate anywhere around the world. Guiora (2017) defines cybersecurity as any measure against criminal conduct committed on or via the internet to deceive, defraud or cause the malfunction of network equipment. Assaults such as computer viruses, distributed denial-of-service attacks, and malware are examples of unlawful activity targeting computer systems. Computer networks and devices may make it easier to commit unlawful conduct, but the aim of the crime is not reliant on the information device or network. Kremling and Parker (2018) explains that cyber security cyberwarfare, cybercrime, cyber terrorism are all the same thing in a document illustrating stake in the military wellbeing of the nation. This is because committing theft or forgery against a specific person or organisation is equivalent to declaring war on the intended victim. There have been changes in the meanings of cybersecurity, cybercrime and cyberspace as technology has progressed through time (Mazurczyk et al., 2016). Mordi (2019) has suggested a description of cybersecurity to highlight the specificity, understanding, or use of information technology since cybercrime encompasses a wide range of crimes.

The internet's limitless expanse is referred to as cyberspace. Several of today's telecommunications systems are based on an interconnected network of information systems components (Meeuwisse, 2015). It is necessary to secure the firm and its users' assets to apply a wide range of tools and policies, including security principles and security protection, guidelines, and risk management methodologies (Noam, 2019). Connected computer devices, staff, infrastructure, applications, services, and telecommunications systems are just a few examples of an organisation's and an individual's digital assets (Mordi, 2019). Cybersecurity aims to guarantee that the security properties of the company and user's assets are protected against relevant cyber threats. The set of guidelines to keep the internet safe is known as cyber-security (Ohwovoriole, 2019). However, as reliance on the internet grows, People are exposed to new dangers. The term cybercrime refers to a group of criminals who target both the internet and the security it provides. Adept cyberattackers and nation-states threaten the economy and national security (Azeez, 2019). For Nigeria's national and economic security, many interconnected and vital structures, technologies, resources, and services are known as cybersecurity are essential. The way we communicate, travel, power our homes, manage our economies, and access government services have all been revolutionised because of the internet.

Defending networks, computers, programs, and data against assaults, damage, or unauthorised access is the goal of cybersecurity (Sule, 2018). The term security in computers or cyberspace refers to cybersecurity. The nation's residents and the nation's communications network must work together to ensure cyber-security. The danger presented by cyber-security breaches is increasing at an outpacing our ability to respond. One part of the breach cannot be ignored or allowed to expand while the other aspects are ignored. As a result, we've concluded that we need to address security vulnerabilities across the board. Crimes committed via technologies and the internet are referred to as cybercrime (Aniekan and Afolabi, 2017). Theft of funds from online bank accounts is only one example of this. Additionally, cybercrime covers non-financial violations, such as infecting other computers with malware or publishing private company information online (Beissel, 2016). When thieves use the internet to collect sensitive information from other Web users, data breaches are the most common kind of cyberattacks.

- *Elements of Cybersecurity*

Defining cyber security means safeguarding networks, processes, and equipment against harm or security breaches by using a variety of security measures against online fraud and theft of personal data (Severo, 2019). In today's world, any information sent via a network may easily be hacked, regardless of personal or professional. Email, audio and video conferencing, Human resource information system, and internet banking are common forms of cybersecurity technologies and communication in the workplace and home (Re-Hashed, 2019). There are a variety of cybersecurity components deployed by organisations and governments working to combat cybercrime, which is why the problem is becoming more and more prevalent (Graham, 2019). Because online transactions account for 60% of all transactions, the information technology sector must prioritise security measures to ensure that customers trade with complete peace of mind. Protecting computers from harmful assaults and illegal access is known as cyber security. Cybersecurity is a critical component for protecting any company or person (Schwanholz & Graham, 2019). The measures of cybersecurity adopted in this study are application security, network security, operational security and information security. According to Babayo et al. (2021), these measures reveal the extent to which cybersecurity is efficiently developed in an environment.

Application security is a critical first step in preventing cyberattacks by including security measures into apps while they are being built. It protects websites and web-based applications against many forms of cyber security attacks that exploit weaknesses in the source code (Sule, 2018). The goal of application security is to prevent software applications from being hacked. Although this is a significant priority for software and cloud service providers, organisations must keep up with the latest developments. Data breaches in cloud accounts are often the result of security settings that were incorrectly configured. Information security refers to cyber security's processes and methodologies for protecting access to sensitive information, usage (Omodunbi et al., 2016), exposure, interruption, alteration, or breaches of security (information theft or information leakage). Personal information, passwords, network information, and social media profiles are examples of data that may be used to identify a person or an organisation (Schwanholz, J., & Graham, 2019). These fundamental information security guidelines are often used in data privacy and regulatory compliance discussions. Information security requirements will be mandatory for the majority of businesses. Failure to meet these criteria might result in heavy fines if someone's personal information is compromised. Cyber security firms will examine how you acquire, store, and transport data. Encryption and security measures will be put in place to guarantee that data is not compromised (Olayemi, 2014). Security of communications networks is another aspect of IT security, guarding against unwanted access to networked systems. Unauthorised access, abuse, and alteration of a computer network and its resources may be prevented and monitored using this collection of rules and settings. It encompasses both software and hardware (Graham, 2019). Network security measures are taken to ensure the safety of the physical network and the devices linked to it. Firewalls are used by most businesses to keep an eye on incoming and outgoing traffic for potential security risks. It's a sort of network protection. Cyber security services enhance network security by securing the wireless connection and making distant connections via encrypted techniques (Pelton & Singh, 2015).

- *Sustainable Peace*

Strategies toward a lasting peace build and improve local capabilities for dealing with the past, engaging in the present, and shaping the future in ways that do not alienate, exploit or discriminate. To put it another way, establishing the conditions for long-term peace requires tearing down the institutions, circumstances, and connections that fuel violence and erecting those that promote it (O'reilly et al., 2015). Very few individuals flatly reject the notion of peace, but as usual, it swiftly loses its meaning when people begin to define what peace is. No matter how peace is characterised as a 'good,' this study contends that its long-term viability depends on the circumstances that allow individuals and corporations to flourish. Negative and positive peace are two of the most common types of peace discussed in peacebuilding literature (O'reilly, 2020). There is no explicit display of actual large-scale violence in a state of negative peace. In Western cultures, the security forces and the justice system are all instances of the state enforcing a negative peace by threatening or using violence (Olaitan, 2018).

People who are continually working together at all levels of society, from local to national, may develop peaceful circumstances via positive rather than negative peace (Garba, 2015). More than merely the exclusion of violence, it is the deliberate establishment of circumstances for the group's peace and wellbeing. According to Osah and Odedina (2017), peacebuilding is an activity that enhances healthy change in society via talk as the main method of conflict transformation. The goal of positive peace is to eliminate or address situations that might lead to violent conflict (Imam et al., 2020). Since conflict situations may be as straightforward or as complicated as they need to be, it is necessary for all parties involved in the dispute to work together to achieve a lasting peace that can be sustained over the long term. A comprehensive view of peace incorporates wellbeing and proper and just interactions and institutions (Iruloh et al., 2017). As a result, the ideals of positive peace entail finding other approaches to conflicts than those found in frameworks of reconciliation, or negative peace, to achieve long-term peace. Violence in any form, institutional, cultural, economic, legal, or physical, cannot be used to achieve lasting peace. While acts of violence may temporarily end a quarrel and restore some semblance of peace, they have a long-term impact on the nature of the relationships between the people involved (Olaitan, 2018). The chances of long-term peace diminish while the drive for further, more violent confrontation increases if the quality of relations between the parties involved in the conflict has deteriorated. As a result of conflicts reactions, the value of the connection between the parties and the disputed topic or item may increase if no violence is employed to resolve the dispute. Transformational space allows parties to develop creative ways to work together that are more likely to benefit everyone (Osah & Odedina, 2017). Peacebuilding via non-violent means is neither a linear process nor a quick fix, but it is a long-term strategy that promotes lasting peace and peacebuilding. As a result, accomplishing a wide variety of sustainable development or sustainability objectives before, during, and after a mine's operation is more likely to be supported by a collective commitment to sustainable peace.

➢ *Theoretical Framework*

This study is anchored on the Cyber power theory. The capacity to utilise cyberspace to produce opportunities and influence change in operational contexts across the mechanisms of power is the definition of cyberpower. The use of cyber power resulted in the development of cyber security (Zhao et al., 2021). Unlike other fields of study, cyber security is a discipline that takes place in the context of an adversary's existence. Precise sciences aid with technological comprehension. Scholarly work in the social sciences may aid in a deeper understanding of the players, but it is seldom used. Technologies and the electronic spectrum are used to produce, store, edit, and share information through networked and linked information assets and telematic networks in the functional realm known as cyberspace (Kateway et al., 2021). Power over others and across mechanisms of power is known as cyber power. Cyberspace may be used to ensure victory and impact other operating settings. It is possible to attain or support national goals by using cyber strategy, which is creating and using cyber-operational capabilities that are connected and integrated with those in other operational domains (Bai et al., 2017). There are new ways of communicating and influencing people throughout the globe because of cyberspace's power.

Over long distances, families utilise the internet to connect in real-time. Through cyberspace, financial firms do worldwide business and commodities deals at the velocity of light. Citizens throughout the globe now have unparalleled access to knowledge, allowing for more awareness and comprehension than ever before (Chen et al., 2018). Aside from all the good it can do for humanity, the cooperative domain is an enormous power source. Cyberspace overshadowed by rivalry and fear is a far cry from a mutually advantageous electronic world. However, this plight is nothing new. That every man should try to achieve peace as far as he has the possibility of doing so, and that if he is unable to, he may explore and exploit all the benefits and aids of conflict is one of Hobbes' basic laws of nature. Civilisation in cyberspace is only going to continue to progress. However, as the domain evolves, so does the elements that want to exercise influence via the internet realm (Zhao et al., 2021).

Cyberpower can transform the way people communicate, collaborate, and even engage in combat. However, it does not eliminate the need for more conventional electricity means. Existing means of military power are augmented and bolstered by cyberspace. Information and performance operations continue to shape the battlefield. Many previously unachievable military objectives are now within reach because of this technology. As a second point, cyber power is a distinct political tool (Sule et al., 2010). Military experts are well-versed in the four pillars of national power: diplomacy, information, military, and economics. Every one of these components may be linked together via cyber power, but it also provides new possibilities. According to the second theory of cyber power, dependency is even more important than military force. As a result, the subject of compulsion is once again brought to the fore. Although he has a significant advantage, he also has a significant weakness. To attain political goals, influential powers are motivated to use cyber power while limiting their susceptibility to the same activities (Ajiji, 2017). Cyber power presents appealing alternatives since it is non-lethal mainly and has a significant impact on countries reliant on the internet. This author disagrees with the predictions of certain soothsayers that cyberspace would fundamentally alter the global environment and the social processes that control it. Protecting air, land, and sea will always be necessary as long as humans rely on them for their entire lives. However, this does not imply that cyber power is weak. Cyber power may be used for political purposes, putting nations that rely on the internet in danger. As with other types of governance, cyber power can influence political choices in the same manner. As military and political officials analyse all aspects of national power, cyber power is an important consideration.

➢ *Empirical Evidence*

According to Kimanuka (2018), countries throughout the globe confront new security threats daily. Terrorism, insurgency, abduction, criminal violence, and sociopolitical insinuations are just a few of the many threats to public safety that may take the form of criminal activity. Progress is severely impeded because countries cannot be at peace without addressing these security issues. According to this, the world's fastest-growing economies experience peace and security since enterprises can be operated out without fear, and investors have the incentive to invest in these countries. Investment in Nigeria would provide more jobs for the country's young, which would lead to a decrease in violence.

For this reason, peacebuilding is critical to the advancement of development. This implies that efforts should be made to end existing armed conflicts around the world to allow for a lasting peace that would offer stability via the assurance of safety.

People's ability to voice their concerns and contribute to the growth of their society is attributed to a lack of human security since it relates to living without fear of instability or violence, whether it is governmental or criminal, social-economic or gender-related. (OSAA 2018). Accessibility to a working security system is another way to convey a person's sense of safety. Individuals' capacities to engage economically, culturally and politically in the advancement of society will be impacted if security is lacking (Office of Special Adviser in Africa, OSAA (2018)). The absence of social violence is not the sole need for a state of peace. Attitude, emotion, and psychology are all involved. Because globalisation and socioeconomic evolution are inextricably linked, the process of establishing peace must be promoted not just in Nigeria but also across the world.

Insurgent organisations are more likely to adopt terrorist activity if they have close relationships with marginalised people and can use media attention of attacks to illustrate their objectives for those who help them commit their violent acts, according to Keels (2018). Insurgent groups are also more plausible in using terrorist activity when they have significant links with political wings, according to Keels (2018). It's a fact of life in Nigeria, where the majority of violent incidents are politically driven. Democratic accountability, according to Grindle (2004), requires revisiting previously successful policies, defining priorities correctly, reviewing policies that directly influence lowering poverty levels, and using creative approaches to putting these policies into action. However, Nigeria is lagging in implementing the positive programs of previous administrations. Rather, the new administration intends to implement new policies that may prove unsuccessful in the long run.

Some of the effective governance measures cited by Rolberg (2014) include poverty alleviation, job creation, a booming economy, safety, health, education, access to clean water, and environmental protection. Kauffman (2002) found causation and positive interactions between different components of democratic accountability and Real per capita GDP income. ' The implication here is that progress is made possible by excellent governance. Participation by disadvantaged and oppressed groups ensures that the marginalised voice may also be heard by the government, allowing for democratic accountability.

According to Lawson (2013), the notion of judicial independence is a critical component of good democratic accountability. Functionaries should always act in the public's best interest rather than their own. The author argues in this passage Social sustainability, according to Kofi Annan, should include respect for the constitution and the rule of law, integrity, openness, sensitivity and public engagement, among other factors. According to Adegbami and Adepoju (2017), information sharing, governance, and involvement in decision-making are necessary for a peaceful, prosperous, and secure society. According to these people, weak governance is the root cause of everything from inequality and underemployment to cyber violence, insurgency, and extremism of all kinds.

Some of the reasons of disputes that contribute to insecurity in Nigeria, according to Ibrahim and Igbuzor (2002), and Osisioma (2016), are as follows: Competition for finite economic and political resources among cultural, religious, and sectional groups; the vilification of faith and cultural fanaticism; and the conversion of national funds into private riches. According to some of the suggestions, the government should constantly focus on finding the fundamental causes of disputes and making the country democratic, rather than the sham democracy that is now practised in Nigeria. It's apparent from Adegbami and Adepoju (2017) statement that corrupt individuals are not excellent leaders. Conflict, bloodshed, terrorism, abduction, criminal violence, and other wrongdoings have left no area of the nation safe, according to the 2016 report by Osisioma.

➢ *The evidence of the empirical literature reveals that there is a need to investigate the interactions between cybersecurity and sustainable peace. In line with this and the research questions raised, the following hypotheses were formulated in the null;*

- Ho1: Operational security does not significantly influence sustainable peace in the Niger Delta region of Nigeria
- Ho2: Network security does not significantly affect sustainable peace in the Niger Delta region of Nigeria
- Ho3: Application security does not significantly affect sustainable peace in the Niger Delta region of Nigeria.
- Ho4: Information security does not significantly drive sustainable peace in the Niger Delta region of Nigeria

III. MATERIAL AND METHOD

A cross-sectional survey design was used in this study in order to identify the relationship among the variables at a given point in time. The study area includes the nine states in the Niger Delta region of Nigeria, which includes Abia, Akwa-Ibom, Bayelsa, Cross River, Delta, Edo, Imo, Ondo and River state. However three states (Rivers, Bayelsa and Edo) states were purposively selected. According to Nigerian Stat (2021), the total number of internet users in the selected state is approximately 26.9 million subscribers. Using the rao soft sample size estimator at 5% margin of error and 99% confidence interval, a sample size of 663 was arrived at. According to Hair et al. (2019), a sample size greater than or equal to 300 is adequate to indraw inferentials. The covenience and volunteer sampling were used to select the respondents for the study in each state. A research questionnaire was used to collect the primary data for this study. The questionnaire was designed based on the research objectives and consists of question items measured on the 5-point likert-scale, ranging from ‘Strongly Agree (5) to ‘Strongly Disagree’ (1). The question items are classified into three sections namely; section A- items on demographic variables, Section B – items on cybersecurity variables and section C – items on sustainable peace variables. A pretest was conducted on the questionnaire, using samples outside the study area, inorder to confirm it's validity and reliability. A Cronbach Alpha statistics of 0.701 was obtained which according to Mugenda and Mugenda (1999) establishes the reliability of the instrument in measuring the study variables.

In line with the cyber power theory and the studies of Babayol et al. (2021) and Sule et al. (2019), simple linear regression models were formulated. have been used to specify the interactions between the dimensions of cybersecurity (operational, network, application and information securities) and sustainable peace. The functional form of the models are specified as follows:

- $SP = \beta_0 + \beta_1(OS) + e$ (1)
- $SP = \beta_0 + \beta_1(NS) + e$ (2)
- $SP = \beta_0 + \beta_1(AS) + e$ (3)
- $SP = \beta_0 + \beta_1(IS) + e$ (4)

➢ *Where:*

- SP - Sustainable Peace
- OP - Operational Security
- NS – Network Security
- AS – Application Security
- IS – Information Security
- β_0 - Intercept Parameter
- β_1 – Regression coefficient
- e – error term of regression

The parameters in the models were estimated through the Ordinary Least Squares (OLS) technique, which captures the relationship between the dependent and independent variables, while avoiding spurious influences. In the Apriori, it is expected that Operational Security, Network Security, Application Security and Information Security will influence Sustainable Peace. The descriptive analysis of the demographic variables were done using frequency tables and perecentages. The inferential analysis includes the serial correlation test, ANOVA test and regression parameter estimates.

IV. RESULT

A total number of four hundred and twenty (420) copies of the questionnaire were properly filled and returned out of a total number six hundred and sity three (663). This represents sixty-three percent (63.3%) response rate. Responses were provided for all the question items in the questionnaire, thus making them useful for the analysis. According to Mugenda and Mugenda (1999), a response rate greater than 50% or equal to 300 is adequate for analysis.

➢ *Demographic Characteristics*

Table 1 shows the result of the analysis of the demographic variables of the repsondents. The results reveals that a total number of 420 respondents completed the questionnaire. The gender distribution shows that 189 (45%) are male and 231 (55%) are female. The age distribution shows a mean age bracket of 31-40years (33.3%) and the occupational distribution indicates that majority of the respondents are self employed (30.7%). Further results suggest that Christianity is a dominant religion in the region (60.7%). The distribution of the state reveals an even spread of the respondents across the nine states in the Niger delta region.

Table 1 Demographic Characteristics of Respondents

Characteristics	Frequency	Percent
Gender		
Male	189	45.0
Female	231	55.0
Ages		
Below 20years	56	13.3
21 – 30years	115	27.4
31 – 40years	140	33.3
41 – 50years	88	21.0
51 – 60years	19	4.5
61years and above	2	0.5
Occupation		
Civil Servant	90	21.4
Private Sector	84	20.0
Self-employed	129	30.7
Student	105	25.0
Others	12	2.9
Religion		
Christian	255	60.7
Muslim	160	38.1
Others	5	1.2
State		
Abia	44	10.5
Akwa-Ibom	48	11.4
Bayelsa	44	10.5
Cross River	46	11.0
Delta	50	11.9
Edo	46	11.0
Imo	45	10.7
Ondo	47	11.2
River	50	11.9

Source: Outputs from SPSS 26 (2022)

- *Decsriptive Statistics*

Table 2 Statistics of Responses to the Study Variables

	N	Minimum	Maximum	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Operational Security	420	1	5	3.80	0.851	-0.611	0.119	0.368	0.238
Network Security	420	1	5	3.85	0.806	-0.610	0.119	0.703	0.238
Application Security	420	1	5	3.55	0.955	-0.320	0.119	-0.316	0.238
Information Security	420	1	5	4.15	0.766	-1.180	0.119	3.071	0.238
Sustainable Peace	420	2	5	4.04	0.773	-0.342	0.119	-0.538	0.238
Valid N (listwise)	420								

Source: Outputs from SPSS 26 (2022)

Table 2 gives the summary of the statistics for the responses to the question items in the questionnaire. The statistics reveals a mean response value of 3.8 for 'Operational Security' (OS) as cybersecurity variable. This mean value implies that majority of the respondents agree with operational security as a component of cybersecurity, with a minimum response value of 1 and maximum of 5. However, this assumption varies across the respondents, with a standard deviation of 85.1 %.

Similarly, there is a mean response value of 3.85 for 'Network Security' (NS), suggesting that the respondents agree with network security as a component variable of cybersecurity in the Niger Delta region. However, a variation of 80.6% indicates a disparity in this assumption across the respondents. Further results also show an average response value of 3.55 for 'Application Security' (AS). This implies that majority of the respondent fairly accept the variable as a component of cybersecurity in their communities. A standard deviation of 95.5% however suggests that this position varies strongly across the respondents.

In addition, ' Information Security' (IS) has a mean response value of 4.15 which suggests that respondents agree with the variable as a component of cybersecurity in the Niger Delta region. The spread (76.6%) implies that this assumption varies among the respondents.

Furthermore, results also reveal that most of the respondents believe that the four components of the cybersecurity variable (OS, NS, AS & IS) influence 'Sustainable Peace' (SP). This is confirmed by the mean response value of 4.04, a minimum value of 2 and maximum value of 5. However, the standard deviation (77.3%) suggests this assumption varies across the respondents.

Lastly, the result of the skewness and kurtosis suggest that the responses to the research instrument are normally distributed across the variables.

- *Regression Diagnostic Test*

Table 3 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	0.370	0.137	0.135	0.719	2.001
2	0.395	0.156	0.154	0.711	1.988
3	0.494	0.244	0.242	0.673	2.093
4	0.317	0.101	0.099	0.734	2.047

Source: Outputs from SPSS 26 (2022)

Tables 3 shows a summary of the regression models in involving the study variables. The results indicate that Operational Security (OP) has a positive relationship with Sustainable Peace (SP) with R coefficient of 0.37. The R-squared value of 0.14 confirms that operational security explains only 14% of the total variations in sustainable peace, in the Niger Delta region of Nigeria. The Durbin-Watson statistics is approximately 2, suggesting that the variables have no serial correlation, and which confirms the absence of autocorrelation between them.

Simillarly, results show a positive association between Network Security (NS) and Sustainable Peace (R = 0.40). However, the R-squared value of 0.16 indicates that network security only account for 16% of the variations in sustainable peace in the Niger Delta region of Nigeria. The Durbin-Watson statistics of 1.99, further suggests the absence of serial correlation between the variables.

Furthermore, the R coefficient of 0.5 reveals an average positive relationship between Application Security (AS) and Sustainable Peace (SP). The R-squared value of 0.24 confirms that application security account for 24% variation in sustainable peace in the Niger Delta region of Nigeria. The Durbin-Watson statistics is approximately 2, indicating the absence of serial correlation between the variables.

In addition, the R coefficient of 0.335 indicate a positive relationship between the dependent and independent variables in the multiple regression model. The R-squared value of 0.126 confirms that the independent variables (data integrity risk, authentication risk and repudiation risk) jointly explain 12.6% of the variations in the dependent variable (internal audit management). The Durbin-Watson statistics of 2.43 also indicate the absence of autocorrelation among the variables.

Table 4 ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	34.314	1	34.314	66.358	0.00
	Residual	216.150	418	0.517		
	Total	250.464	419			
2	Regression	39.119	1	39.119	2.104	0.00
	Residual	211.345	418	0.506		
	Total	250.464	419			
3	Regression	61.115	1	61.115	4.971	0.00
	Residual	189.350	418	0.453		
	Total	250.464	419			
4	Regression	25.241	1	25.241	3.362	0.00
	Residual	225.223	418	0.539		
	Total	250.464	419			

Source: Outputs from SPSS 26 (2022)

Table 4 reveals the ANOVA results of the model effect of the variables. The F-statistics (F=66.36) of the model 1 (operational security and sustainable peace) is statistically significant at the 5% level (p-value = 0.00). Similar results hold for model 2 (network security and sustainable peace), model 3 (application security and sustainable peace) and model 4 (information security and sustainable peace) with F-statistics of 2.10, 4.97 and 3.36 respectively. These values are all statistically significant at the 5% level (p-value = 0.00).

- Regression Estimates and Hypotheses Testing
- *Hypothesis 1:*

  Ho1: Operational security does not significantly influence sustainable peace in the Niger Delta region of Nigeria

Table 5 Parameter Estimates of Model 1

Model 1		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.757	0.161		17.147	0.03
	Operational Security	0.336	0.041	0.370	8.146	0.01

Source: Outputs from SPSS 26 (2022)

The positive regression coefficient in Table 5 ($\beta_1 = 0.37$) implies a direct relationship between Operational Security (OS) and Sustainable Peace (SP), where a unit change in OS drives SP by 37% . The t-statistics of the regression co-efficient (t = 8.15) is statistically significant at the 5% statistical level (p = 0.01). From this result, the null hypothesis is rejected and it is concluded that operational security significantly influence sustainable peace in the Niger Delta region of Nigeria.

- *Hypothesis 2:*

  Ho2: Network security does not significantly influence sustainable peace in the Niger Delta region of Nigeria

Table 6 Parameter Estimates of Model 2

Model 2		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.574	0.170		15.166	0.02
	Network Security	0.379	0.043	0.395	8.796	0.02

Source: Outputs from SPSS 26 (2022)

The positive regression coefficient in Table 6 ($\beta_1 = 0.40$) reveals a direct relationship between Network Security (NS) and Sustainable Peace (SP), where a unit change in NS results in 40% change in SP. The t-statistics of the regression co-efficient (t = 8.80) is statistically significant at the 5% statistical level (p = 0.02). Therefore, the null hypothesis is rejected and it is concluded that network security significantly influence sustainable peace in the Niger Delta region of Nigeria.

- *Hypothesis 3:*
  Ho3: Application security does not significantly influence sustainable peace in the Niger Delta region of Nigeria

Table 7 Parameter Estimates of Model 3

Model 3		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.618	0.126		20.711	0.00
	Application Security	0.400	0.034	0.494	11.615	0.03

Source: Outputs from SPSS 26 (2022)

The positive regression coefficient in Table 7 ($\beta_1 = 0.49$) implies a direct relationship between Application Security (AS) and Sustainable Peace (SP), where a unit change in AS drives SP by 49%. The t-statistics of the regression co-efficient (t = 11.62) is statistically significant at the 5% statistical level (p = 0.03). Hence, the null hypothesis is rejected and it is concluded that application security significantly influence sustainable peace in the Niger Delta region of Nigeria.

- *Hypothesis 4:*
  Ho4: Information security does not significantly influence sustainable peace in the Niger Delta region of Nigeria

Table 8: Parameter Estimates of Model 4

Model 4		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.708	0.197		13.732	0.02
	Information Security	0.320	0.047	0.317	6.844	0.00

Source: Outputs from SPSS 26 (2022)

The positive regression coefficient in Table 8 ($\beta_1 = 0.32$) shows a direct relationship between Information Security (IS) and Sustainable Peace (SP), where a unit change in IS implies 32% change in SP. The t-statistics of the regression co-efficient (t = 6.84) is statistically significant at the 5% statistical level (p = 0.00). Therefore, the null hypothesis is rejected and it is concluded that information security significantly influence sustainable peace in the Niger Delta region of Nigeria.

V. SIMMARY OF FINDINGS AND IMPLICATIONS

The study was conducted to investigate the impact of cybersecurity on on sustainable peace in the nIger Delta region of Nigeria. The findings has revealed that cybersecurity measures significantly influence sustainable peace. Specifically, the study has shown that there exist a positive relationship between operational security and sustainable peace; network security and sustainable peace; application security and sustainable peace; and information security and sustainable peace. The result shows that operational security is a significant driver of sustainable peace. That is, in achieving sustainable peace, it is necessary to identify vital information that may be beneficial to security agencies and other stakeholders and then take steps to prevent or minimize the use of that information by the enemy. The findings corroborate the positions of Sule (2018) and Ajiji (2017) that a security and risk management technique should specify the types of information that must be protected from unauthorized access and misuse in aother to have a better society. The findings aslo reveal that network security significantly drives peace in the Niger Delta. The implication of this is that sustainable peace might not be achieved when people with unauthorised access can track friendly activities on when critical actions to avoid or reduce their use of the essential information has not being put in place. The findings support the position of Azeez (2019); Chen et al. (2019) and Keels (2018) that identifying the kinds of information that need to be secured is the first step in a vulnerability management strategy which could bring aboutsecurity of lives and propertites. The importance of network security extends to both personal and commercial networks.

Furthermore, the analysis reveals the interaction between application security and sustainable peace in the Niger Delta. This implies that when application security increases, sustainable peace also increases. This adds credence to the works of Katew et al. (2021) that when it comes to ensuring software safety in innovation, the whole application development lifecycle must be considered and that the long-term objective is to enhance the security procedures of organizations so that problems with apps may be found, fixed and ideally avoided in future. The findings also establish that information security is key to the sustainability of peace in the Niger Delta. It's all a part of keeping an eye on potential threats to sensitive data. Unauthorized exploitation, exposure, interruption, alteration, observation, retention, or destruction of information prevention is the primary goal of information security.

VI. CONCLUSION

The study investigates the interactions between cyber security and peace in the Niger Delta region of Nigeria. Anchored on the cyber power theoy the study establishes that the dimensions of cybersecurity (Operational Security, Network Security, Application Security and Information Security) significantly drives Sustainable Peace. The majority of households with high-speed connectivity have one or more internet connections that might be abused if they are not adequately protected. Data loss, piracy, and manipulation may all be reduced with the aid of a reliable network security system. It is the process of building, implementing, and testing data encryption in programs to avoid security problems against attacks such as unapproved access or manipulation. A queue manager's interface triggers security services when an application connects to the queue manager. End-to-end security and message-level security are other terms for application-level security. The study recommends robust actions should be taken by stakeholders and government agencies in protecting critical cyber infrastructures in aother to achieve and sustain peace in the Niger Delta.

REFERENCES

[1]. Adegbami, A. and Adepoju, B.K. (2017). Good Governance in Nigeria: A Catalyst to National Peace, Stability and Development. AFRREV 11(4) 144-155

[2]. Ajiji, Y. M. (2017). Cybersecurity Issues in Nigeria and Challenges. International Journal of Advanced Research in Computer Science and Software Engineering 7(4): 315–321

[3]. Aniekan, M. N., & Afolabi, M. B. (2017). “Introduction to Cybersecurity and Cybercrime.” In Aniekan & Afolabi (Eds.) Intelligence and Security Studies Programme. Lagos, Nigeria: Spectrum

[4]. Antonucci, D. (2017). The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities. Hoboken, NJ: John Wiley & Sons.

[5]. Azeez, O. (2019). “Cybercrime Cost Nigeria N288 bn in 2018.” Business a.m. https://www.businessamlive.com/cyber-crime-cost-nigeria-n288bn-in-2018/, accessed March 25, 2020.

[6]. Babayol, S., Bakri, M., Usman, S., Mohammed, Muhammed, M. (2021). Cybersecurity and cybercrime in Nigeria: The implications on national security and digital economy. Journal of Intelligence and Cyber Security , 4(1),

[7]. Bai, C.-Z., Pasqualetti, F., Gupta, V.: Data-injection attacks in stochastic control systems: detectability and performance tradeoffs. Automatica 82, 251–260 (2017)

[8]. Beissel, S. (2016). Cybersecurity Investments: Decision Support under Economic Aspects. Geneva: Springer.

[9]. Buchanan, B. (2016). The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations. New York: Oxford University Press

[10]. Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. Journal of Information Security and Applications, 42, 36–45. doi:10.1016/j.jisa.2018.08.002

[11]. Cavelty, M. D., & Wenger, A. (2019). “Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science.” Contemporary Security Policy 41(1): 1–28.

[12]. Chen, Y., Kar, S., Moura, J.M.F.: Optimal attack strategies subject to detection constraints against cyber-physical systems. IEEE Trans. Control Netw. Syst. 5(3), 1157–1168 (2018)

[13]. Chukwuma, O. A. I., & Mogom, I. A. (2018). “The Internet and National Security in Nigeria: A Threat-Import Discourse.” Covenant University Journal of Politics & International Affairs 6(1): 20–29

[14]. Diogenes, I., & Ozkaya, E. (2018). Cybersecurity Attacks and Defense Strategy. Birmingham, UK: Packt Publishers

[15]. Garba, G.K (2015) Building Women’s Capacity for Peace building in Nigeria. Review of History and Political Science June 2016, Vol. 4, No.1, 31-46.

[16]. Global Cybersecurity Index (2019). 2019 Global Cybersecurity Index. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

[17]. Graham, M. (2019). “Changing Connectivity and Digital Economies at Global Margins.” In Graham (Ed.) Digital Economies at Global Margins. Cambridge, MA: The MIT Press

[18]. Grindle, M. (2004). “Good enough governance. Poverty reduction and reform in developing countries.” Governance 17 (3) 525-548

[19]. Guiora, A. M. (2017). Cybersecurity, Geopolitics and Law. London: Routledge.

[20]. Ibrahim, J. and Igbuzor, O. (2002). “Memorandum submitted to the Presidential Committee on National Security in Nigeria

[21]. Imam, A., Hauwa, B., and Yahi, M. (2020). Women’s Informal Peacebuilding in North East Nigeria. Bergen: Chr. Michelsen Institute (CMI Brief no. 2020:09) p6.

[22]. Iruloh Betty- Ruth N. and Uche Chineze M. (2017) Role of Women in Conflict Resolution and Peacebuilding inn Niger Delta Region of Nigeria. International Journal of Social Sciences, Vol 5(4).

[23]. Katewa V., Bai CZ., Gupta V., Pasqualetti F. (2021) Detection of Attacks in Cyber-Physical Systems: Theory and Applications. In: Ferrari R.M., Teixeira A.M.H. (eds) Safety, Security and Privacy for Cyber-Physical Systems. Lecture Notes in Control and Information Sciences, vol 486. Springer, Cham. https://doi.org/10.1007/978-3-030-65048-3_5

[24]. Keels, E. (2018). Explaining the puzzle of Rebel terrorism in oefresearch.org. (Online). Available July 2019

[25]. Kimanuka, O. (2018). Why peace and security of development essential enablers of development https://www.newtimes.co.rw/opinons/pe ace-security-development

[26]. Koops, B. (2016). “Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research.” In Akhgar, B., & Brewster, B. (Eds.) Combating Cybercrime and Cyberterrorism: Challenges, Trends and Priorities. Geneva: Springer.

[27]. Kosseff, J. (2017). Cybersecurity Law. Hoboken, NJ: John Wiley & Sons.

[28]. Kremling, J., & Parker, A. M. S. (2018). Cyberspace, Cybersecurity and Cybercrime. London: Sage.

[29]. Kshetri, N. (2019). "Cybercrime and Cybersecurity in Africa." Journal of Global Information Technology Management 22(2): 77–81

[30]. Lawson, R. (2012). "Book Review of BO Rothstein: The Quality of Government: Corruption, Social Trust and Inequality in International Perspective". Public Choice 150 (3-4), 793-795

[31]. Mazurczyk, W., Drobniak, C., & Moore, S. (2016). "Towards a Systematic View on Cybersecurity Ecology." In Akhgar, B., & Brewster, B. (Eds.) Combating Cybercrime and Cyberterrorism: Challenges, Trends and Priorities, 17–38. Geneva: Springer.

[32]. Mordi, M. (2019). "Is Nigeria Really the Headquarters of Cybercrime in the World?" Guardian. https://guardian.ng/news/is-nigeria-really-the-headquarters-of-cybercrime-in-the-world/. Accessed March 25, 2020

[33]. Noam, E. M. (2019). Managing Media and Digital Organisations. New York: Palgrave Macmillan. Ohwovoriole, O. (2019). "Nigeria Losses About N127bn to Cybercrime Annually." ThisDay. https://allafrica.com/stories/201906190144.html. Accessed March 25, 2020

[34]. Pelton, J. N., & Singh, I. B. (2015). Digital Defense: A Cybersecurity Primer. Cham: Springer.

[35]. Olayemi, O. J. (2014). "A Socio-Technological Analysis of Cybercrime and Cyber Security in Nigeria." International Journal of Sociology and Anthropology 6(3): 116–125.

[36]. Omodunbi, B. A., Odiase, P. O., Olaniyan, N., & Esan, A. O. (2016). "Cybercrimes in Nigeria: Analysis, Detection and Prevention." FUOYE Journal of Engineering and Technology 1(1): 37–4

[37]. Olaitan, Z. (2018). Women's Participation in Peace Processes in Nigeria; Challenges and Prospects. Available Online: https://www.researchgate.net/publication/328216329

[38]. O'Reilly, M., Súlleabháin, A., and Paffenholz, T. (2015) Re-Imagining Peacemaking: Women's Roles in Peace Processes. New York: International Peace Institute.

[39]. Office of the Special Adviser of Africa (OSAA) (2018). Peace and Security for development https://www.government.se/49b74d/onte ntasets/036c986985e04c32beee05a913b cc/9/ (Online). Available 20 October, 2018

[40]. Osah, G. and Odedina A. (2017). Women as Factor in Peacemaking and Peacebuilding in the Niger Delta Region. International Journal of Development Research, 7(3), 11987-11993.

[41]. Osisioma, B.C. (2016). Conflict Management and Peace Building in Nigeria. https://www.researchgate.net/MANAGE MENT-AND-PEACE-BUILDING-INNIGERIA-FINMG-TITE-COMMONGROUND/PDF

[42]. Re-Hashed. (2019). Cybercrime Statistics: A Closer Look at the "Web of Profit. www.thesslstore.com. Accessed March 25, 2020

[43]. Rotberg, R. (2014). "Good governance means performance and results". Governance, 27(3) 511-518.

[44]. Schwanholz, J., & Graham, T. (2018). "Digital Transformation: New Opportunities and Challenges for Democracy." In Schwanholz, J. & Graham, T. (Es.) Managing Democracy in the Digital Age: Internet Regulations, Social Media Use, and Online Civic Engagement. Geneva: Springer.

[45]. Severo, M. (2019). "Safeguarding without a Record? The Digital Inventories of Intangible Cultural Heritage." In Romele, A., & Terrone, E. (Eds.) Towards a Philosophy of Digital

[46]. Sule, B. (2018). Political party financing and election reformations in Nigeria's 2015 general election: issues and impacts. PhD Thesis submitted to the School of International Studies, College of Law Government and International Studies, Ghazali Shafie Graduate School of Government, Universiti Utara Malaysia

[47]. Sule, B. Yahaya, M.A. Rabi'u, A.A. Ahmad, M. & Hussaini, K. (2019). "Strategies of Combating Insurgency in Northeastern Nigeria: A Non-Traditional Approach." Journal of Administrative Studies 16(2): 54–75

[48]. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems, 1–16. doi:10.1080/08874417.2020.171226

[49]. Zhao, Z., Ye, R., Zhou, C., Wang, D., & Shi, T. (2021). Control-theory based security control of cyber-physical power system under multiple cyber-attacks within unified model framework. Cognitive Robotics, 1, 41–57. doi:10.1016/j.cogr.2021.05.001